HOUSE OF REPRESENTATIVES
2 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0002
(207) 287-1400
TTY: Maine Relay 711

Margaret O'Neil
21 Sheila Circle
Saco, ME 04072
Phone: (207) 590-1679
Margaret.O'Neil@legislature.maine.gov

May 22, 2023

Testimony of Rep. Maggie O'Neil sponsoring

LD 1902, An Act to Protect Personal Health Data

Before the Joint Standing Committee on Judiciary

Good afternoon, Senator Carney, Representative Moonen, and members of the Judiciary Committee, I am Maggie O'Neil. I represent House District 129 in Saco. Thank you for the opportunity to present **LD 1902, An Act to Protect Personal Health Data.**

This bill will close gaps in current law protecting health data. To draft the bill, I used the "My Health, My Data Act," which recently passed in the state of Washington.[1]

Health data has fewer safeguards than we expect. Because we often hear references to HIPAA on doctor's office forms or on the news, many of us assume that the federal Health Information Portability and Accountability Act (HIPAA) law protects all of our private health data.

The reality is different. HIPAA, enacted in 1996, was largely concerned with issues like helping us maintain health insurance when we change jobs. HIPAA does lays out privacy rules for health care providers and insurance companies to follow when they handle our personally identifiable medical data. However, the same piece of information that is protected at a doctor's office can be totally unregulated in other settings. We should have strong protections for all sensitive health data, but the law hasn't caught up.

Right now, your health data has certain protections when you are at the doctor's office. You do not have those same protections when dealing with an entity not covered by HIPPA. Examples include health data collected by apps (e.g., mental health or period tracking app), wearable devices (e.g., Apple Watch or FitBit), and web searches (e.g., WebMD). This bill will close that gap in law to give us better information and control over what happens to our health data.

Potential harms range from unwanted advertising to discrimination and even prosecution. Risks include loss of control, stigma, and loss of safety and security. Examples include:

---

[1] WA HB 1155.

a. Targeted ads.
b. Data breaches revealing identifiable personal information.
c. Health apps often provide enough information to make users completely identifiable, even if they don't share names or other identifiers with third parties. We lack transparency about how companies such as insurance providers might use this data in discriminatory ways, even if it is not legal to use it. Access to this data is taking place far from public view without accountability.
d. Make access to medical care more unequal: e.g., algorithms used to determine which patients need care (such as patient risk of mortality, likelihood of readmission, and in-home care needs).
e. Digital redlining: Data can be packaged, analyzed, and sold to be used to make decisions about you, from whether someone should rent to you, hire you, lend you money, or give you benefits.
f. Criminal prosecution: In a state where abortion or gender-affirming care is outlawed, an entity might report information to law enforcement if a person is suspected of having an abortion or seeking gender-affirming care. As states restrict access to abortion, people may fear that seeking guidance on ending a pregnancy, or even getting treatment during a miscarriage, might lead to unwanted attention from the police, prosecutors, or individuals who take matters into their own hands. Fear, harassment, and criminalization create significant barriers between patients and the care they need.

Everyone should be able to access the health care they need without their personal health information being collected and shared without their permission or knowledge.

What the bill does: Safeguards for consumer health data

This bill would require entities to comply with certain safeguards when handling with consumer health data, including:

1. **Disclose health information that is collected and shared**: Entities must tell consumers (a) what health data they collect about them; (b) how they collect that health data (identify sources); (c) why the health data is collected; and (d) what health data they share with third parties and whom they share it with. A consumer may request confirmation from a company on whether the company is collecting or sharing their health data. The request process must be accessible so that consumers don't need to jump through extra hoops.
2. **Consent required to collect and share consumer health data:** Consent may not be obtained by deceptive means. Consent will not be required when data use or sharing is "strictly necessary" to provide a product or service that the consumer requests. Also, a consumer may request that a company delete the consumer's existing health data.

3. **Data security requirements:** An entity handling health data must take reasonable steps to protect health data. They must restrict who can access the health data (employees, service providers, and contractors only for purposes consented to or requested by the consumer). They must maintain reasonable data security practices relative to the data being processed.
4. **Ban on sale of health data:** Health data is especially sensitive. We should discourage health data markets to avoid harmful discrimination, fear of accessing care, and prosecution.
5. **Prohibition on geofencing:** Geofencing may not be used around health care facilities for the purpose of identifying, tracking, collecting data from, or sending notifications or messages to a person that enters the facility. In 2022, Vice uncovered a story about a data broker charging just $160 to purchase a week's worth of data identifying people who visited Planned Parenthood, where they came from, and where they went afterwards.[2]

Health data protections ensure better health outcomes. We are more likely to get the medical care we need when we feel safe seeking care and information. To feel safe, we need to be able to make choices about how our health data is tracked, used, and sold. On top of this, the *Dobbs* decision and bills across state legislatures restricting access to abortion and gender-affirming care have raised serious concerns that the data collected by apps and websites could be used to target or arrest people accessing health care. Until we enact this law, few protections exist to prevent companies from collecting, retaining, or disclosing this personal information to third parties.

Health data is sensitive data that requires a high level of protection and security. This bill goes upstream to prevent harm before it occurs. The principles behind this project are (a) data privacy and (b) data minimization. Data privacy involves choice and control about how your data is collected and what is done with it (e.g., notice and consent requirements). It is necessary for personal autonomy. Data minimization avoids collecting sensitive and unnecessary data at the front end to prevent harm. It's a data management principle that encourages data handlers to limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose. Smart data managers are encouraged to practice data minimization as part of privacy by design.[3]

---

[2] "Data broker sells location data of people who visit abortion clinics." May 2022. https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.

[3] *See* "Privacy By Design Resources" International Association of Privacy Professionals (IAPP) https://iapp.org/resources/article/oipc-privacy-by-design-resources/. *See* also "Quality Data Only: How to Apply Data Minimization to Your Business." (March 2023) https://www.business.com/articles/how-to-apply-data-minimization/.

This bill is about giving us choices. Some people will want to opt-in to targeted advertising, and other people will not. That is for each of us to decide. The most important thing we can do as lawmakers is ensure that we can make those decisions for ourselves as Mainers.

Thank you.

Figure 1: Is your health data protected?

Activity	Protected by HIPAA?
Browsing the web for health info, e.g.: a. using Psychology Today to find a therapist; b. visiting Drugs.com to learn how your medications interact; c. using WebMD to look up cardiac symptoms; d. YouTubing medical advice about preventing diabetes; or e. shopping for pregnancy tests online.	No. Normally, a website can monetize your data however it likes, as long as it follows its own privacy policy and terms of service.
Wearing a smart watch (Fitbit, Apple, Garmin), e.g.,: a. Heart rate data; b. Sleep quality; c. Fitness tracking; d. Gait measurements that reveal a health condition or disability.	No. You are only covered by the terms of service for Fitbit, Apple, or Garmin.
Using apps that store and interpret data, e.g.: a. Mental health, mood, and meditation apps (e.g., a screening checklist for depression); b. Weight loss apps; c. Substance use supports; d. Prescription trackers; or e. Period or fertility trackers.	No, unless the app is acting on behalf of a provider (e.g., MyChart). In 2020, Consumer Reports found that all popular period trackers tested shared very personal data with other companies for advertising purposes. Companies are allowed to list themselves as HIPAA compliant, even if they have determined the law doesn't apply to them.

Talking to a doctor	Yes. HIPAA lays out strict guidelines for interactions with doctors, clinics, dentists, psychologists, nursing homes, hospitals, and other healthcare providers. You're also protected during telemedicine appointments on platforms such as Doxy.me, Vsee, and Zoom for Healthcare. The same goes for their "business associates" – e.g., billing companies and online patient portals. Most of the time, those entities are barred from using identifiable health information for anything other than research, billing, insurance, and providing care unless they have your permission.
Talking to your health insurance company	Yes. The same privacy protections you expect at a doctor's office are in operation for health insurance companies. However, HIPAA doesn't apply to other kinds of insurance (e.g., if a life insurance company acquires information about your health, it's not required to safeguard it the way HIPAA-covered entities are). Workplace wellness programs aren't always covered by HIPAA, even if you get a discount on your health insurance for participating. Coverage depends on factors including whether the program is being run by your health insurer, your employer, or a company hired just to administer the program.

Bringing your phone to a medical clinic	No. Data brokers glean location information from phones and purchases that can show where people travel, whether to a gym, a mental health clinic, a church, or an abortion provider. In 2022, Vice reported that, for just $160, reporters were able to purchase a week's worth of location data for people who visited reproductive healthcare clinics, including information on where the individuals had traveled from, and where they went afterwards.

Source: Consumer Reports, 2022. https://www.consumerreports.org/health-privacy/guess-what-hipaa-isnt-a-medical-privacy-law-a2469399940/

Current Law: HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established nationwide standards for using, disclosing, storing, and transferring protected health information (PHI). PHI is individually identifiable health information that relates to an individual's past, present, or future physical or mental health or condition, or to the provision of health care to the individual.

HIPAA applies to (a) "covered entities," which are health care providers, health plans, and health care clearinghouses, and (b) "business associates," which are entities that perform certain functions or activities that involve the use or disclosure of protected health information on behalf of a covered entity. Covered entities and business associates subject to HIPAA must have an individual's authorization to use or disclose PHI unless a specified exception applies. Some authorization exceptions pertain to disclosures for treatment, payment, and health care operations, research purposes, law enforcement purposes, and public health activities.